ORACLE®

What's New in Oracle Identity Manager 12c PS3

Arda Eralp
Middleware Consultant

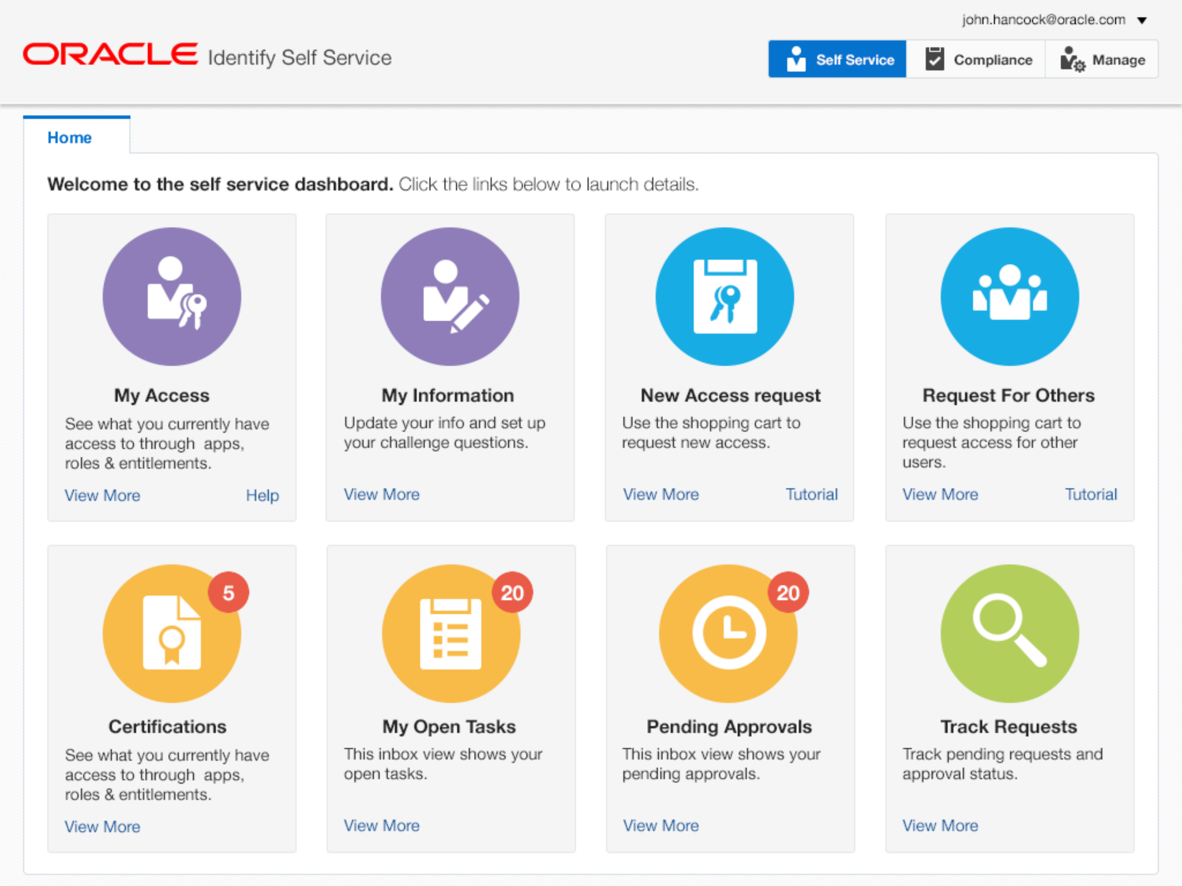
Agenda

- User Interface
- Administration
- Role Life Cycle Management
- Identity Audit / Segregation of Duties
- Audit and Reporting

User Interface

User Interface

Continued UI Simplification



Welcome to the self service dashboard. Click the links below to launch details.

My Access
See what you currently have access to through apps, roles & entitlements.
View More Help

My Information
Update your info and set up your challenge questions.
View More

New Access request
Use the shopping cart to request new access.
View More Tutorial

Request For Others
Use the shopping cart to request access for other users.
View More Tutorial

Certifications 5
See what you currently have access to through apps, roles & entitlements.
View More

My Open Tasks 20
This inbox view shows your open tasks.
View More

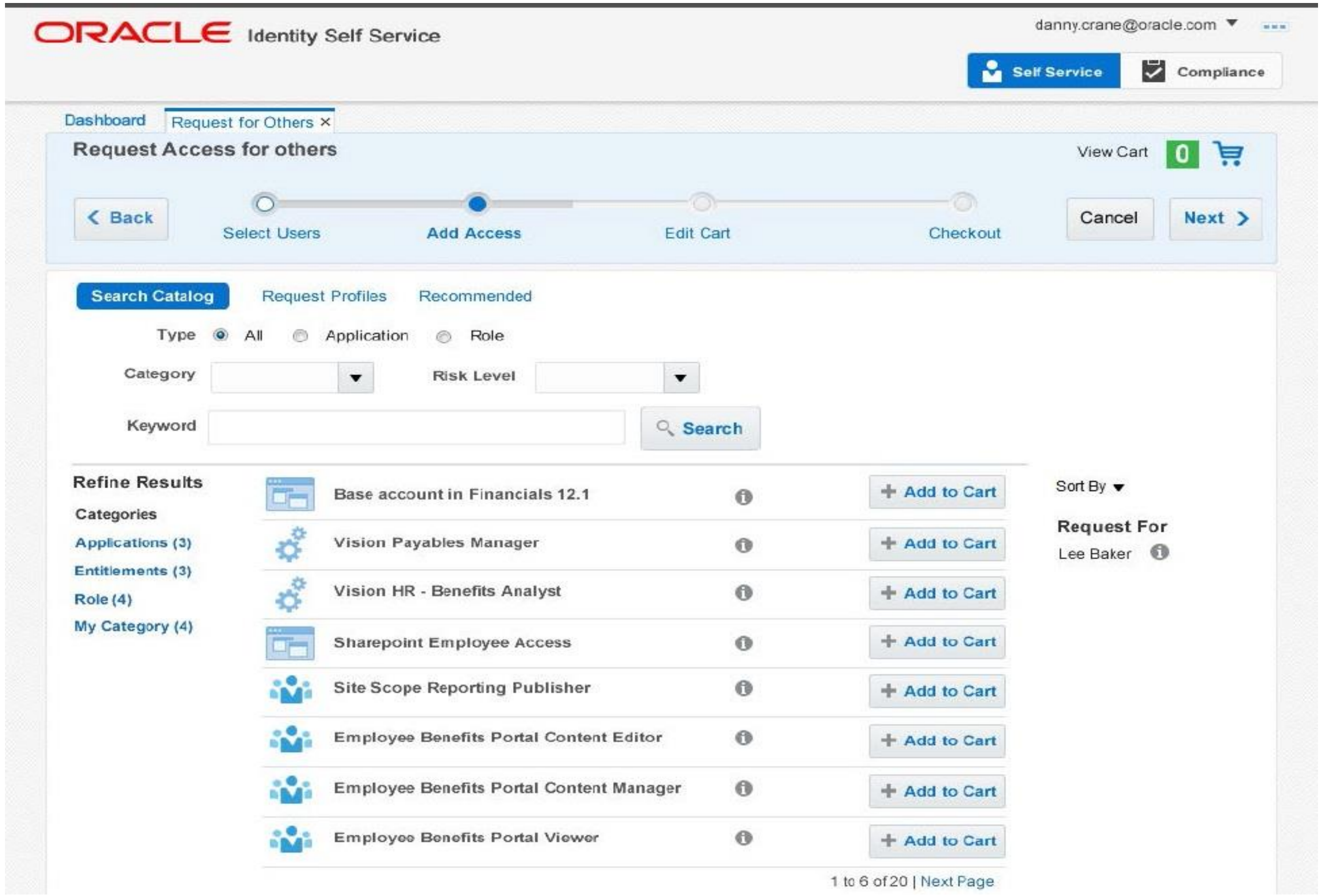
Pending Approvals 20
This inbox view shows your pending approvals.
View More

Track Requests
Track pending requests and approval status.
View More

- Cleaner UI with a Cloud look and feel, with faster performance
- Tablet-Friendly

User Interface

Guided Access Catalog (Shopping Cart Paradigm)



Request Access for others

Type ● All ○ Application ○ Role

Category ▾ Risk Level ▾

Keyword

Refine Results

Categories

- Applications (3)
- Entitlements (3)
- Role (4)
- My Category (4)

Base account in Financials 12.1	+ Add to Cart
Vision Payables Manager	+ Add to Cart
Vision HR - Benefits Analyst	+ Add to Cart
Sharepoint Employee Access	+ Add to Cart
Site Scope Reporting Publisher	+ Add to Cart
Employee Benefits Portal Content Editor	+ Add to Cart
Employee Benefits Portal Content Manager	+ Add to Cart
Employee Benefits Portal Viewer	+ Add to Cart

Request For
Lee Baker

1 to 6 of 20 | Next Page

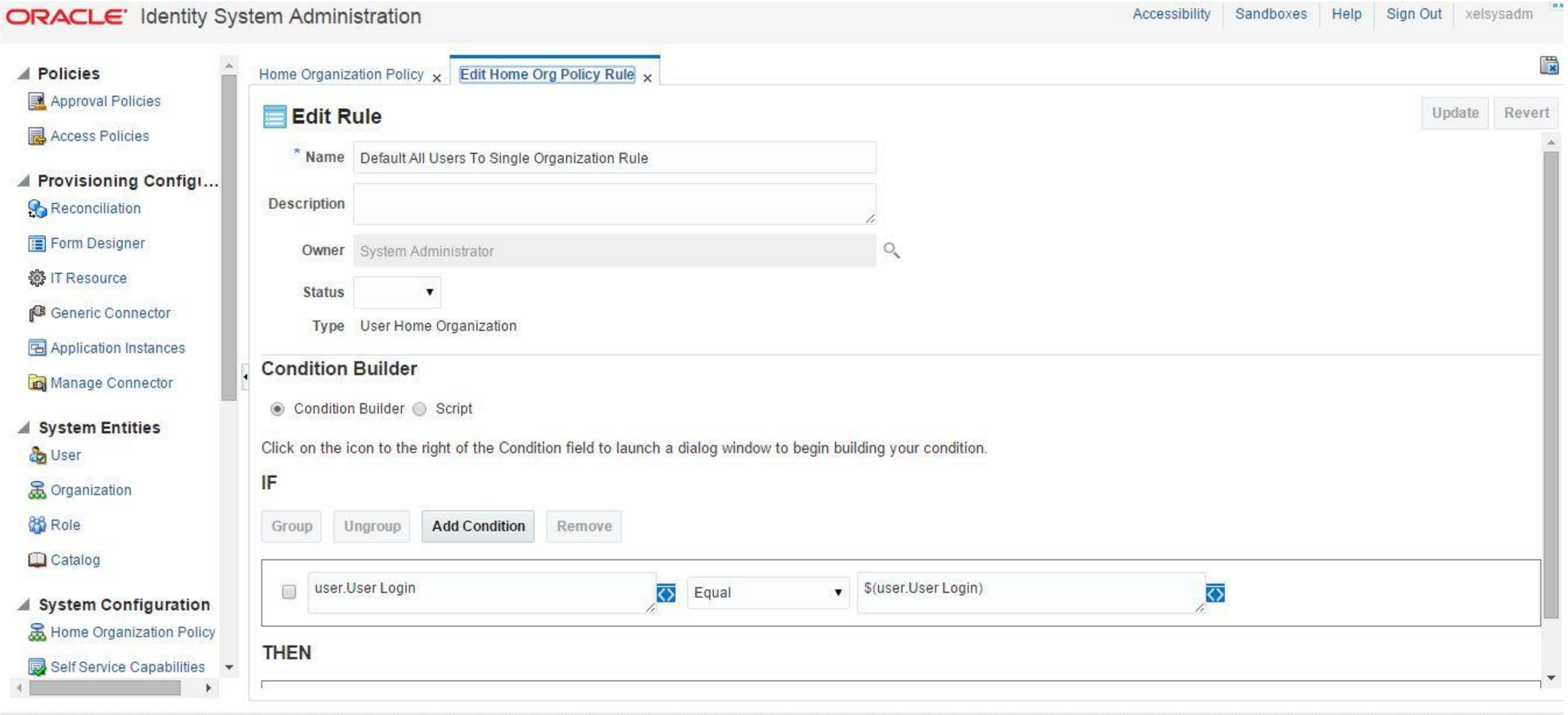
- Business-friendly Access Catalog
- Search, Browse And Contextual Recommendations
- In-line Policy Checks To Prevent SOD Violations
- Flexible Forms For Advanced Data Capture
- End-to-end Visibility Into The Approval And Fulfillment Process

Administration

Administration

Concept of a Home Organization

- A user will be automatically added to an organization based on Home Organization Policy.



Edit Rule

* Name: Default All Users To Single Organization Rule

Description:

Owner: System Administrator

Status:

Type: User Home Organization

Condition Builder

● Condition Builder ○ Script

Click on the icon to the right of the Condition field to launch a dialog window to begin building your condition.

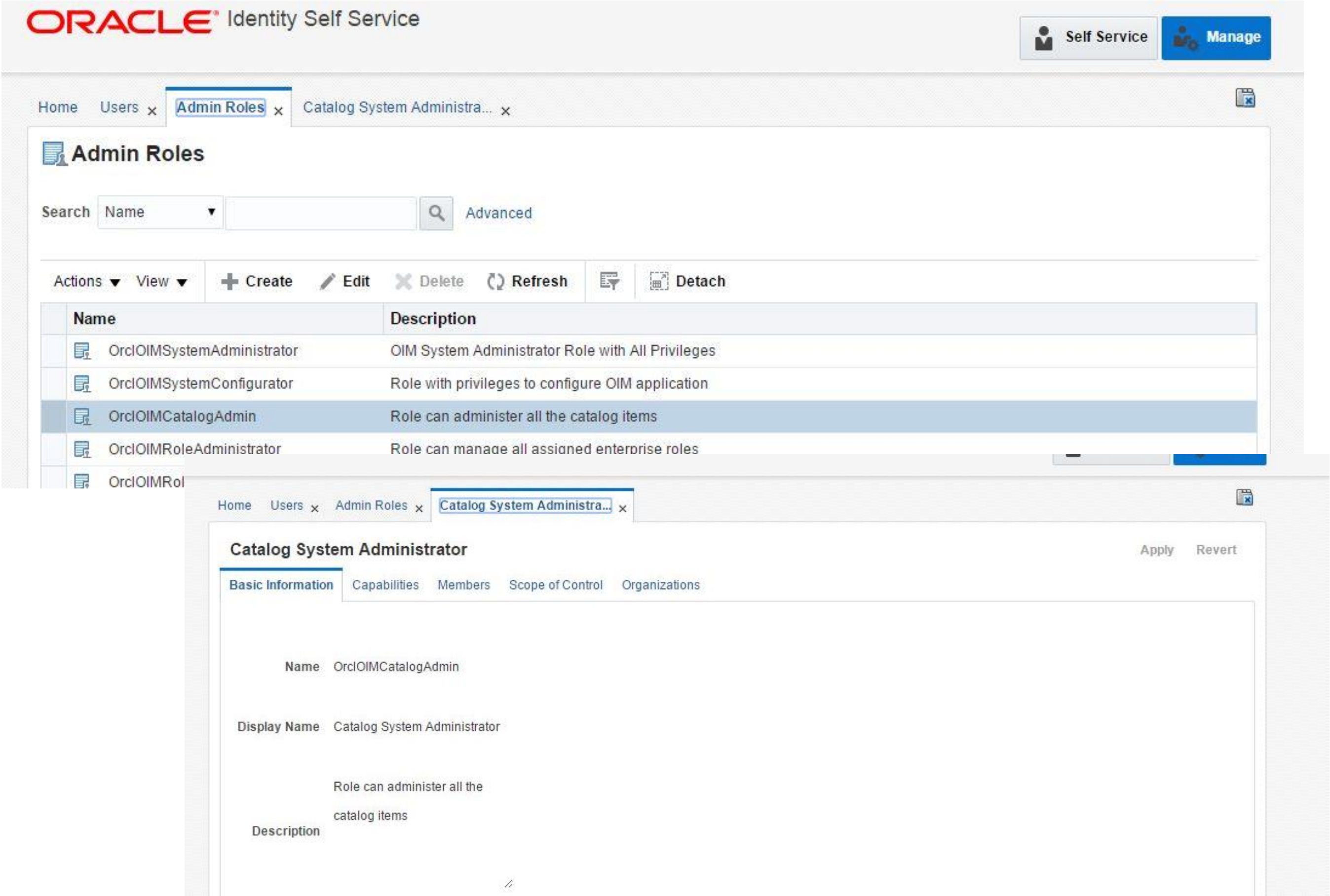
IF

□ user.User Login | Equal | $(user.User Login)

THEN

Administration

Custom Admin Roles



Admin Roles

Search Name ▾ Advanced

Name	Description
OrclOIMSystemAdministrator	OIM System Administrator Role with All Privileges
OrclOIMSystemConfigurator	Role with privileges to configure OIM application
OrclOIMCatalogAdmin	Role can administer all the catalog items
OrclOIMRoleAdministrator	Role can manage all assigned enterprise roles
OrclOIMRol	

Catalog System Administrator

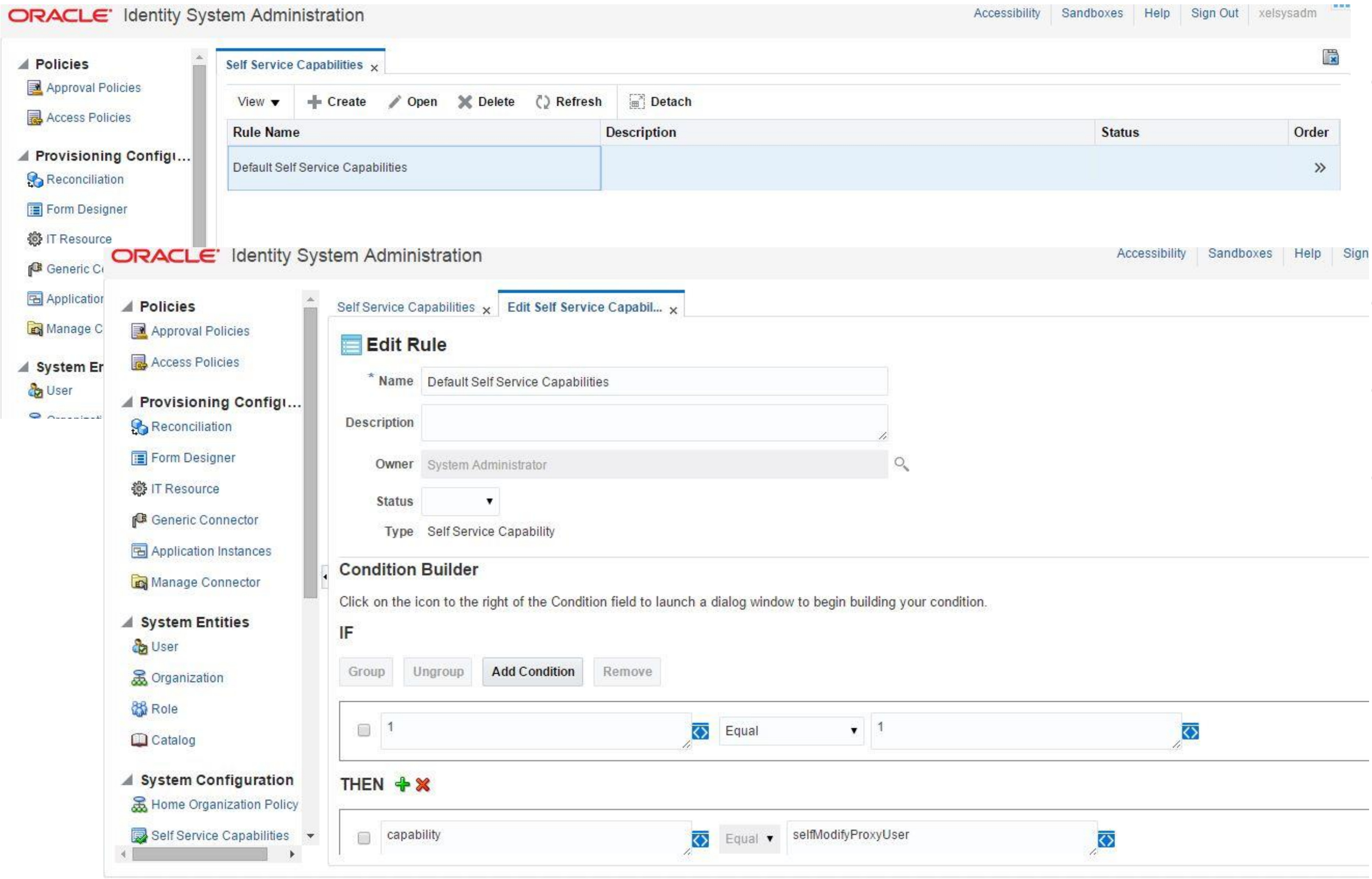
Name OrclOIMCatalogAdmin

Display Name Catalog System Administrator

Description Role can administer all the catalog items

- More dynamic in nature as opposed to static Admin Roles in previous versions.

Administration
Self Service Capability Policy



Rule Name	Description	Status	Order
Default Self Service Capabilities			»

Edit Rule

* Name: Default Self Service Capabilities

Description:

Owner: System Administrator

Status:

Type: Self Service Capability

Condition Builder

Click on the icon to the right of the Condition field to launch a dialog window to begin building your condition.

IF

□ 1 Equal 1

THEN

□ capability Equal selfModifyProxyUser

- Rules within this policy would help determine what operations can a user perform on his own profile.
- This is also driven by user attributes
- No dependency on OES
- Grants for New and Existing Access

Role Life Cycle Management

Role Life Cycle Management

What is it?

- Roles provide a powerful abstraction layer to help scale Identity Management infrastructure by providing access rights grouping mechanism
- Contains system and privileges
- Makes assignments based on job function
- Provides mechanism for detecting violations

ORACLE

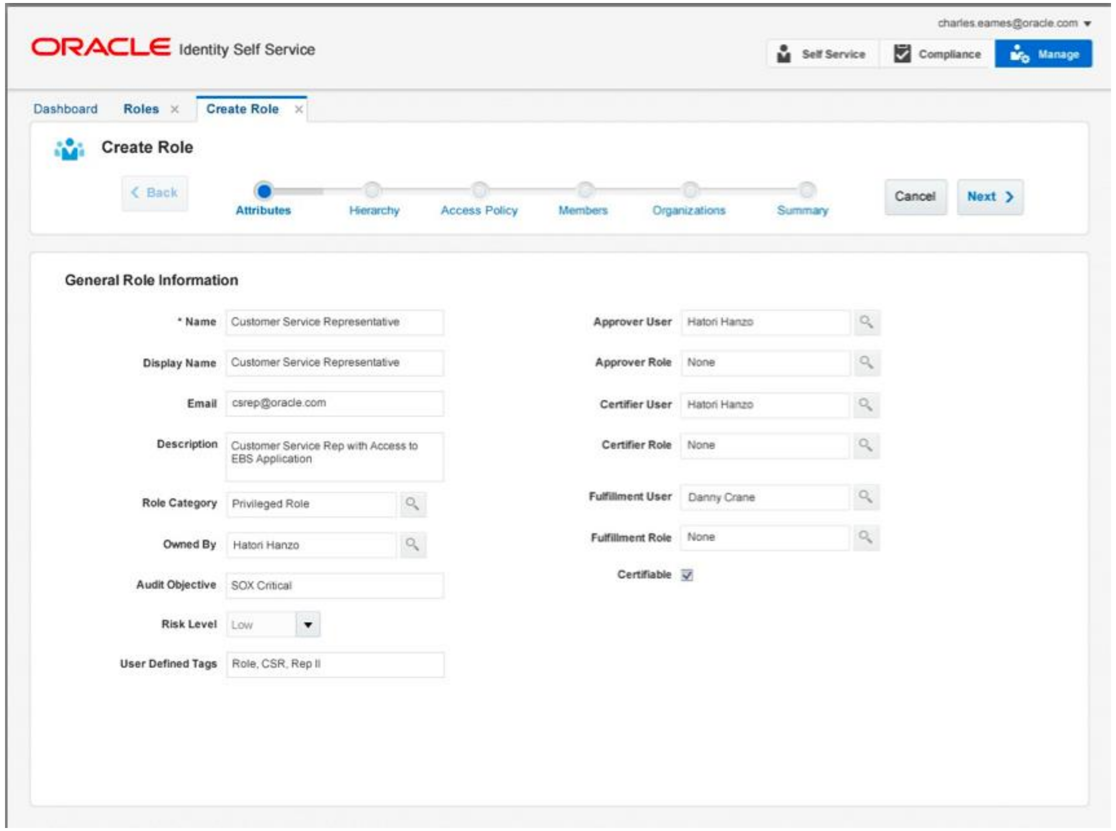
Role Life Cycle Management

Benefits

- Provides an understandable model for access
- Provides an efficient definition of process and policies
- Reduces auditing efforts
- Provides a common language between business and information technology
- Provides consistent, known controls for defining access
- Facilitate access requests more easily

Role Life Cycle Management

Comprehensive Role Lifecycle Management



General Role Information

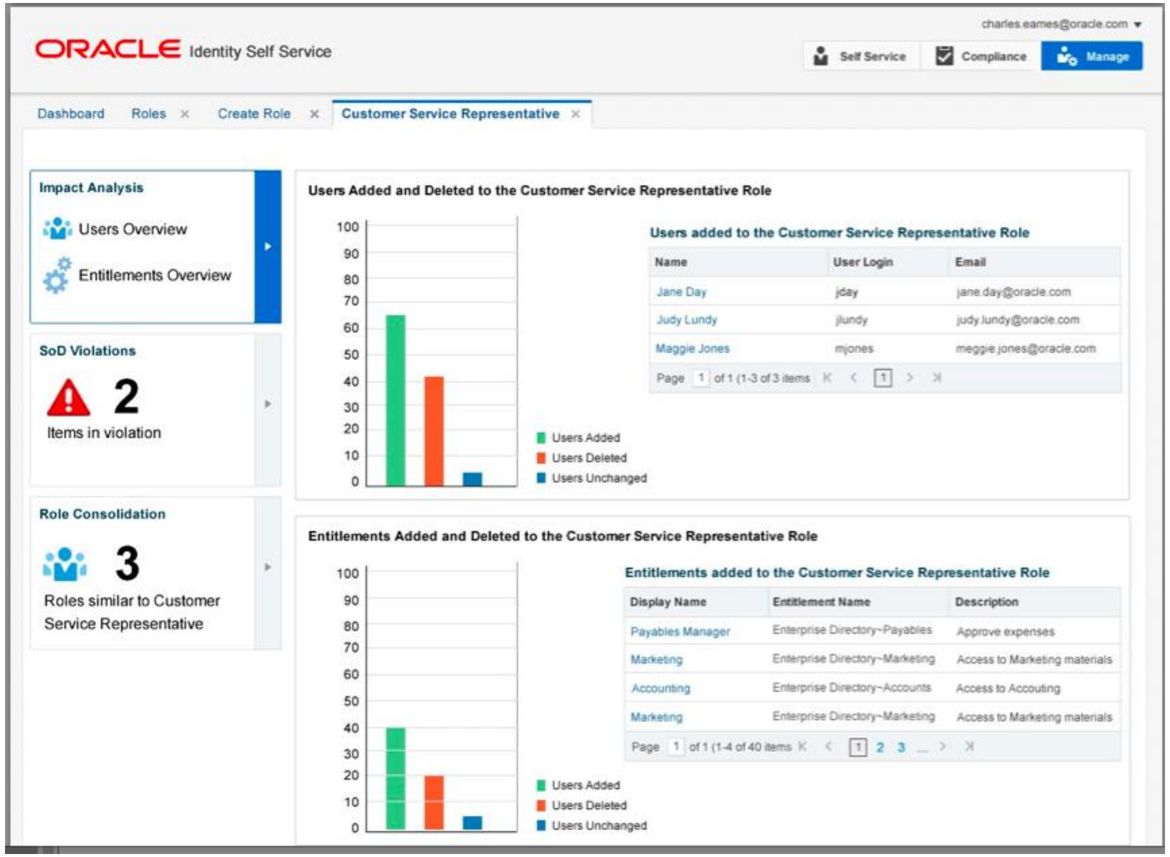
* Name	Customer Service Representative
Display Name	Customer Service Representative
Email	csrep@oracle.com
Description	Customer Service Rep with Access to EBS Application
Role Category	Privileged Role
Owned By	Hatori Hanzo
Audit Objective	SOX Critical
Risk Level	Low
User Defined Tags	Role, CSR, Rep II

Approver User	Hatori Hanzo
Approver Role	None
Certifier User	Hatori Hanzo
Certifier Role	None
Fulfillment User	Danny Crane
Fulfillment Role	None
Certifiable	☑

- Business users can request creation of new roles and changes to existing ones
- Role requests can leverage the same request and approval framework available for Access Requests and Certification
- Role owners can see comprehensive auditing

Role Life Cycle Management

Role Analytics



Users Added and Deleted to the Customer Service Representative Role

Users added to the Customer Service Representative Role

Name	User Login	Email
Jane Day	jday	jane.day@oracle.com
Judy Lundy	jlundy	judy.lundy@oracle.com
Maggie Jones	mjones	meggie.jones@oracle.com

Page 1 of 1 (1-3 of 3 items

Entitlements Added and Deleted to the Customer Service Representative Role

Entitlements added to the Customer Service Representative Role

Display Name	Entitlement Name	Description
Payables Manager	Enterprise Directory~Payables	Approve expenses
Marketing	Enterprise Directory~Marketing	Access to Marketing materials
Accounting	Enterprise Directory~Accounts	Access to Accouting
Marketing	Enterprise Directory~Marketing	Access to Marketing materials

Page 1 of 1 (1-4 of 40 items 1 2 3 ...

- Comprehensive role analytics allows business users to see the impact of new roles and changes to existing ones
- Role owners can reduce role explosion by review the effectiveness of the roles and consolidate new roles with existing ones
- Business users can create roles using “model users”

Identity Audit / Segregation of Duties

Identity Audit / Segregation of Duties

What is it?

- A control process designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task
- Identity Audit (IDA) is used to:
  - Detect combinations of privileges held by users or roles that can lead to access violations
  - Determine policy violations and their causes
  - Detect and act upon Segregation of Duties (SoD) violations

Access Review

JDOE	Accounts Payable	✓
JDOE	Accounts Receivable	⊘

Identity Audit / Segregation of Duties

Benefits

- Prevent /detect fraud and risk
- To provide assurance that transactions/process are Valid and incompliance with rules and regulations

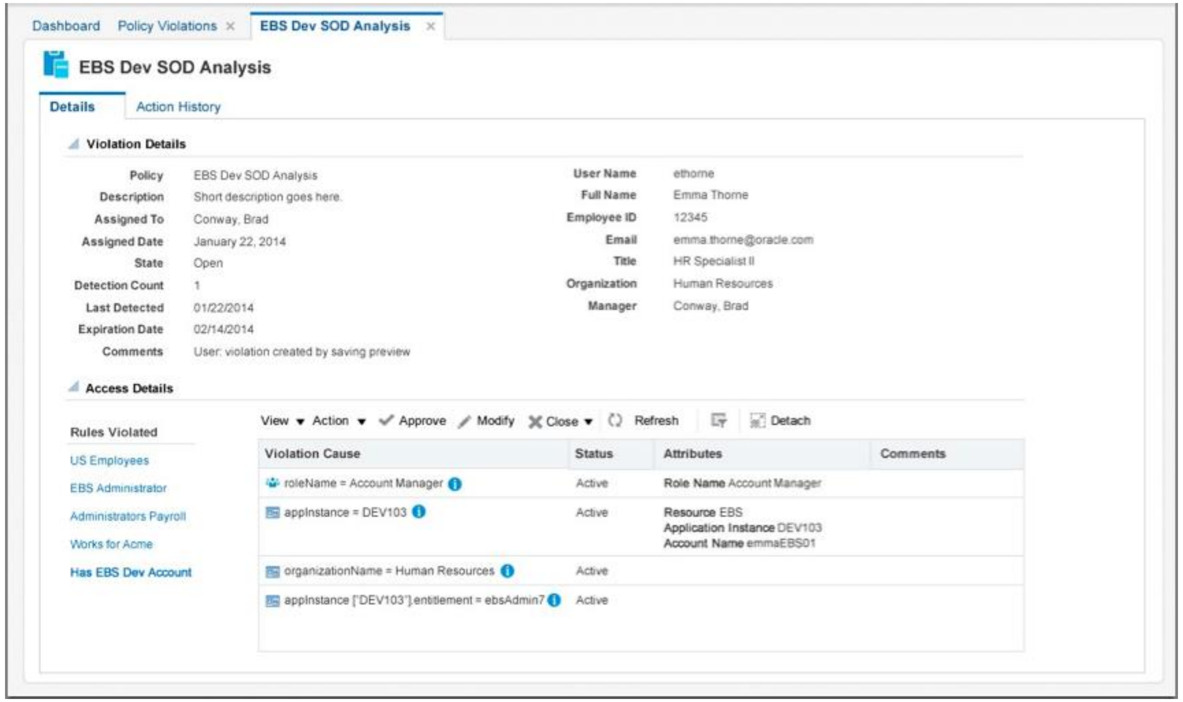
Access Review

JDOE	Accounts Payable	✓
JDOE	Accounts Receivable	⊘

ORACLE

Identity Audit / Segregation of Duties

SOD Detection and Closed Loop Remediation



EBS Dev SOD Analysis

Violation Details

Policy	EBS Dev SOD Analysis	**User Name**	ethorne
Description	Short description goes here.	**Full Name**	Emma Thorne
Assigned To	Conway, Brad	**Employee ID**	12345
Assigned Date	January 22, 2014	**Email**	emma.thorne@oracle.com
State	Open	**Title**	HR Specialist II
Detection Count	1	**Organization**	Human Resources
Last Detected	01/22/2014	**Manager**	Conway, Brad
Expiration Date	02/14/2014		
Comments	User: violation created by saving preview		

Access Details

Rules Violated

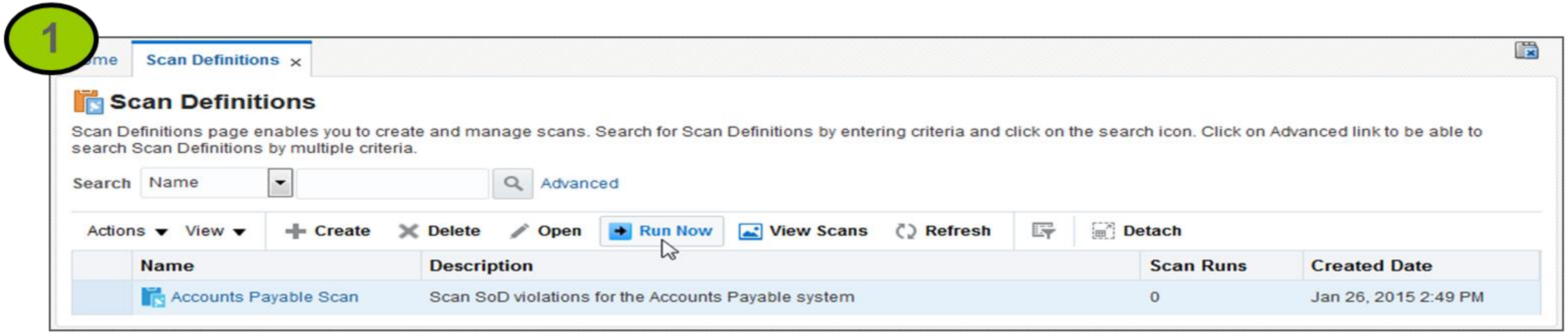
- US Employees
- EBS Administrator
- Administrators Payroll
- Works for Acme
- Has EBS Dev Account

Violation Cause	Status	Attributes	Comments
roleName = Account Manager	Active	**Role Name** Account Manager	
appInstance = DEV103	Active	**Resource** EBS **Application Instance** DEV103 **Account Name** emmaEBS01	
organizationName = Human Resources	Active		
appInstance ["DEV103"].entitlement = ebsAdmin7	Active		

- SOD Rule and Policy Definition
  - Define rules across users, applications, roles and entitlements
- Detective SOD Analysis
  - Detective Policy Enforcement – Closed Loop Remediation
  - Access History to audit all violations and decisions
  - Review High Risk policy violations in Certifications
- Preventative SOD Analysis
  - Enforce SOD policies during access requests
  - Review policy violations during approvals and launch exception workflows

Identity Audit / Segregation of Duties

Detective IDA: Running and Viewing Scan Definitions



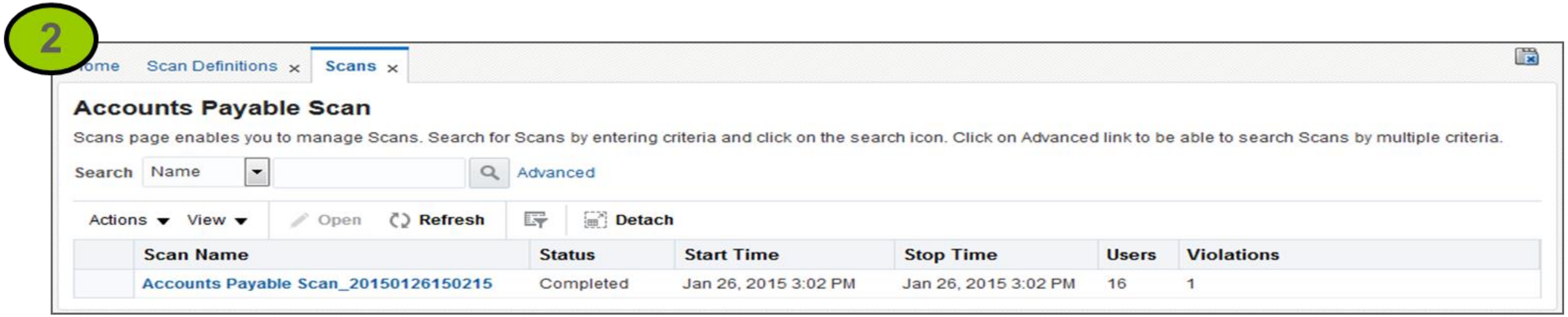
1

Scan Definitions

Scan Definitions page enables you to create and manage scans. Search for Scan Definitions by entering criteria and click on the search icon. Click on Advanced link to be able to search Scan Definitions by multiple criteria.

Search: Name

	Name	Description	Scan Runs	Created Date
	Accounts Payable Scan	Scan SoD violations for the Accounts Payable system	0	Jan 26, 2015 2:49 PM



2

Accounts Payable Scan

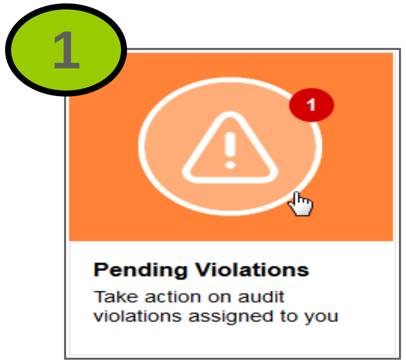
Scans page enables you to manage Scans. Search for Scans by entering criteria and click on the search icon. Click on Advanced link to be able to search Scans by multiple criteria.

Search: Name

	Scan Name	Status	Start Time	Stop Time	Users	Violations
	Accounts Payable Scan_20150126150215	Completed	Jan 26, 2015 3:02 PM	Jan 26, 2015 3:02 PM	16	1

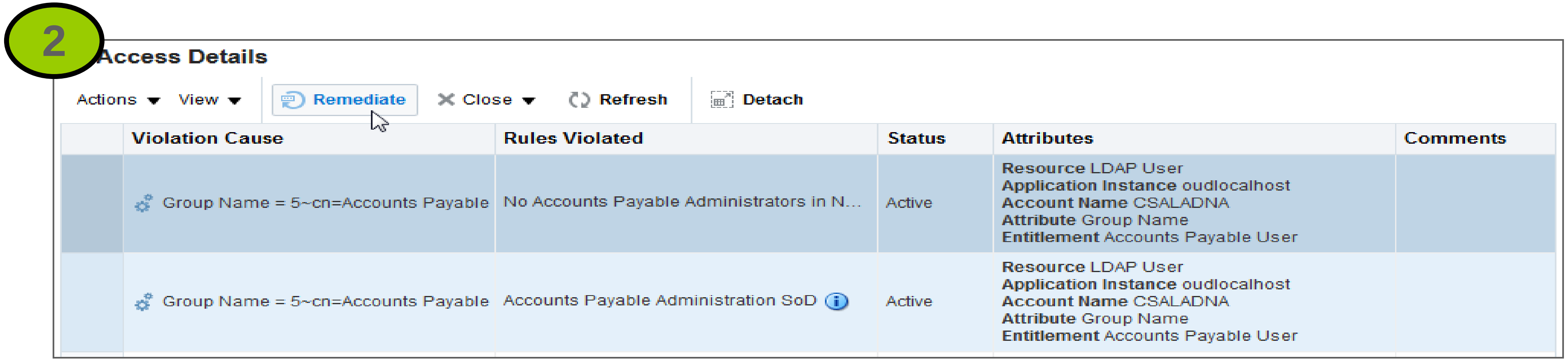
Identity Audit / Segregation of Duties

Detective IDA: Remediate Violations



Pending Violations

Take action on audit violations assigned to you

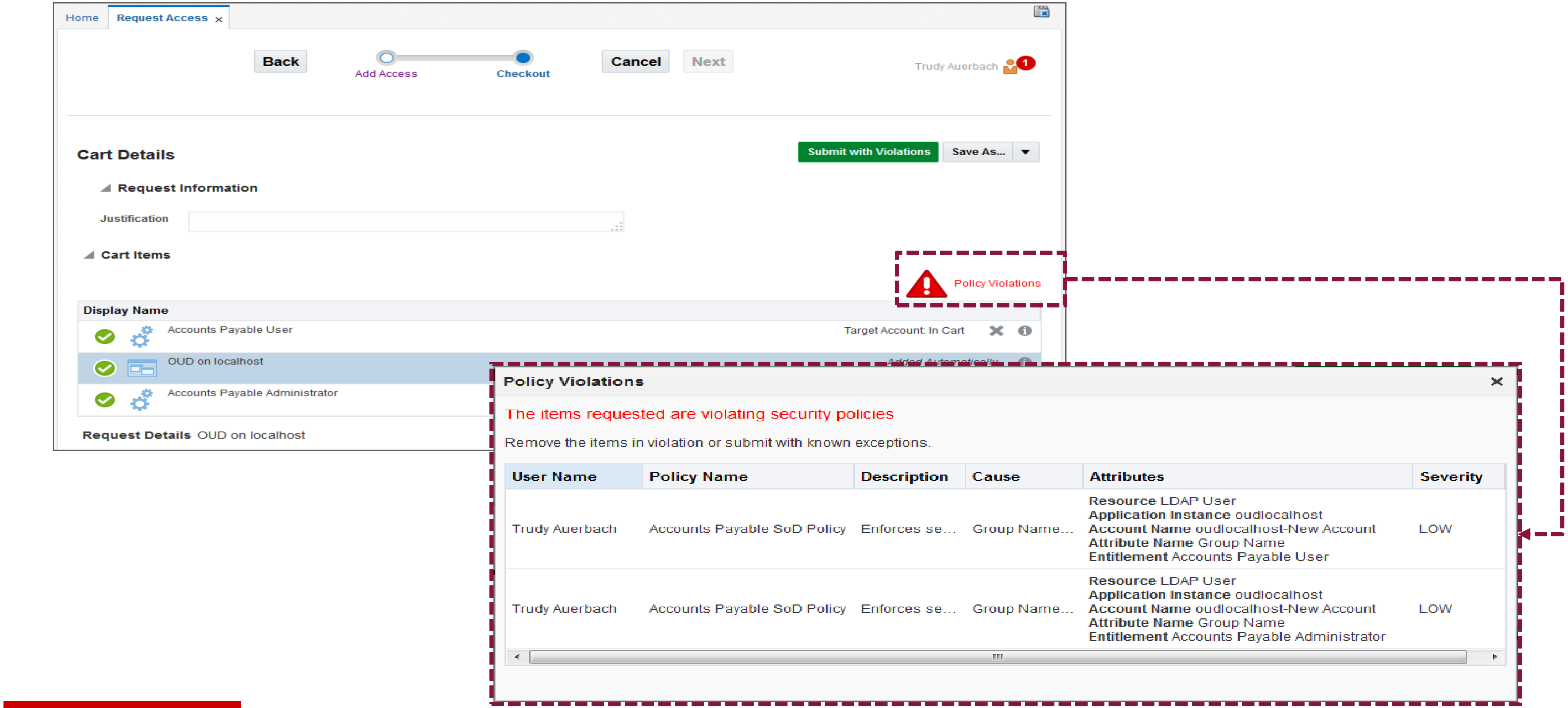


Access Details

	Violation Cause	Rules Violated	Status	Attributes	Comments
	Group Name = 5~cn=Accounts Payable	No Accounts Payable Administrators in N...	Active	**Resource** LDAP User **Application Instance** oudlocalhost **Account Name** CSALADNA **Attribute** Group Name **Entitlement** Accounts Payable User	
	Group Name = 5~cn=Accounts Payable	Accounts Payable Administration SoD	Active	**Resource** LDAP User **Application Instance** oudlocalhost **Account Name** CSALADNA **Attribute** Group Name **Entitlement** Accounts Payable User	

Identity Audit / Segregation of Duties

Preventative IDA: During request



Cart Details

Request Information

Justification

Cart Items

Display Name		
✓ Accounts Payable User	Target Account: In Cart	✕ ⓘ
✓ OUD on localhost	Added Automatically	ⓘ
✓ Accounts Payable Administrator		

Request Details OUD on localhost

Policy Violations ✕

The items requested are violating security policies

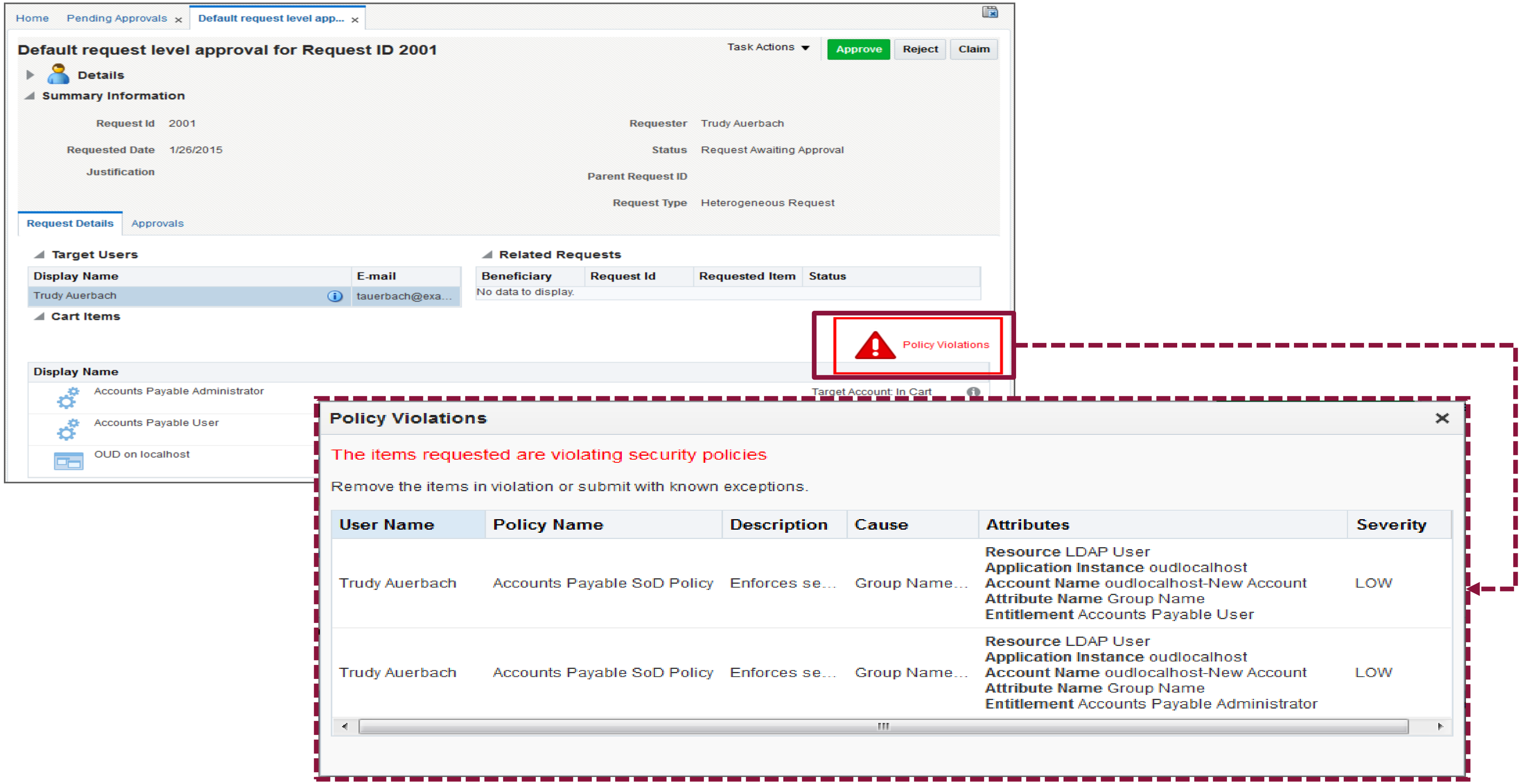
Remove the items in violation or submit with known exceptions.

User Name	Policy Name	Description	Cause	Attributes	Severity
Trudy Auerbach	Accounts Payable SoD Policy	Enforces se...	Group Name...	**Resource** LDAP User **Application Instance** oudlocalhost **Account Name** oudlocalhost-New Account **Attribute Name** Group Name **Entitlement** Accounts Payable User	LOW
Trudy Auerbach	Accounts Payable SoD Policy	Enforces se...	Group Name...	**Resource** LDAP User **Application Instance** oudlocalhost **Account Name** oudlocalhost-New Account **Attribute Name** Group Name **Entitlement** Accounts Payable Administrator	LOW

ORACLE

Identity Audit / Segregation of Duties

Preventative IDA: During approval



Default request level approval for Request ID 2001

▸ **Details**

◢ **Summary Information**

Request Id	2001	Requester	Trudy Auerbach
Requested Date	1/26/2015	Status	Request Awaiting Approval
Justification		Parent Request ID	
		Request Type	Heterogeneous Request

◢ **Target Users**

Display Name	E-mail
Trudy Auerbach	tauerbach@exa...

◢ **Related Requests**

Beneficiary	Request Id	Requested Item	Status
No data to display.			

◢ **Cart Items**

Display Name	
Accounts Payable Administrator	Target Account: In Cart
Accounts Payable User	
OUD on localhost	

Policy Violations ✕

The items requested are violating security policies

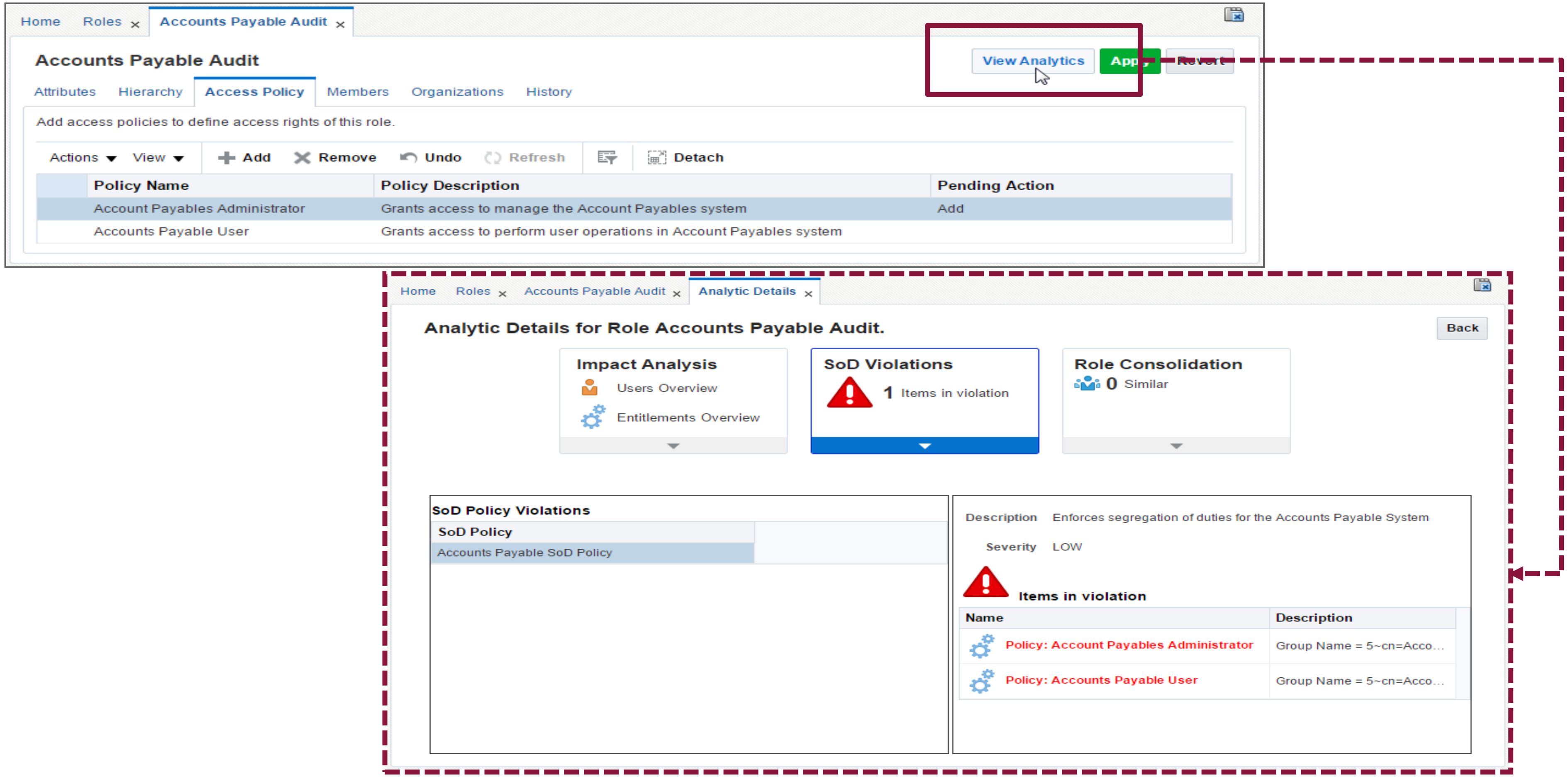
Remove the items in violation or submit with known exceptions.

User Name	Policy Name	Description	Cause	Attributes	Severity
Trudy Auerbach	Accounts Payable SoD Policy	Enforces se...	Group Name...	**Resource** LDAP User **Application Instance** oudlocalhost **Account Name** oudlocalhost-New Account **Attribute Name** Group Name **Entitlement** Accounts Payable User	LOW
Trudy Auerbach	Accounts Payable SoD Policy	Enforces se...	Group Name...	**Resource** LDAP User **Application Instance** oudlocalhost **Account Name** oudlocalhost-New Account **Attribute Name** Group Name **Entitlement** Accounts Payable Administrator	LOW

ORACLE®

Identity Audit / Segregation of Duties

IDA and Role Analytics



Accounts Payable Audit

Add access policies to define access rights of this role.

Policy Name	Policy Description	Pending Action
Account Payables Administrator	Grants access to manage the Account Payables system	Add
Accounts Payable User	Grants access to perform user operations in Account Payables system	

Analytic Details for Role Accounts Payable Audit.

SoD Policy Violations

SoD Policy
Accounts Payable SoD Policy

Description Enforces segregation of duties for the Accounts Payable System

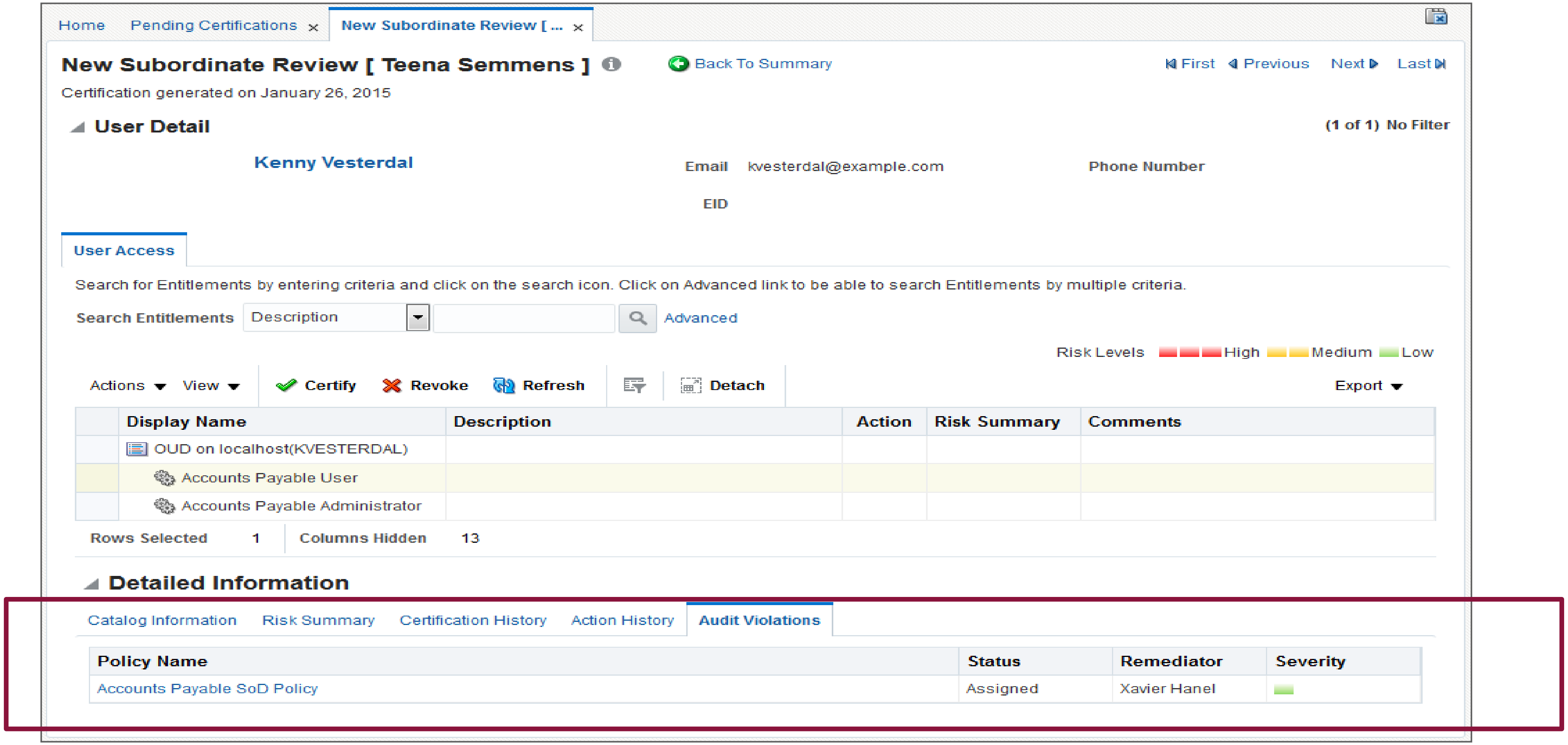
Severity LOW

Items in violation

Name	Description
Policy: Account Payables Administrator	Group Name = 5~cn=Acco...
Policy: Accounts Payable User	Group Name = 5~cn=Acco...

Identity Audit / Segregation of Duties

IDA during Certification review



New Subordinate Review [Teena Semmens]

Back To Summary

First | Previous | Next | Last

Certification generated on January 26, 2015

User Detail

(1 of 1) No Filter

Kenny Vesterdal

Email	kvesterdal@example.com
Phone Number	
EID	

User Access

Search for Entitlements by entering criteria and click on the search icon. Click on Advanced link to be able to search Entitlements by multiple criteria.

Search Entitlements: Description

Advanced

Risk Levels 🟥🟥🟥 High 🟨🟨 Medium 🟩 Low

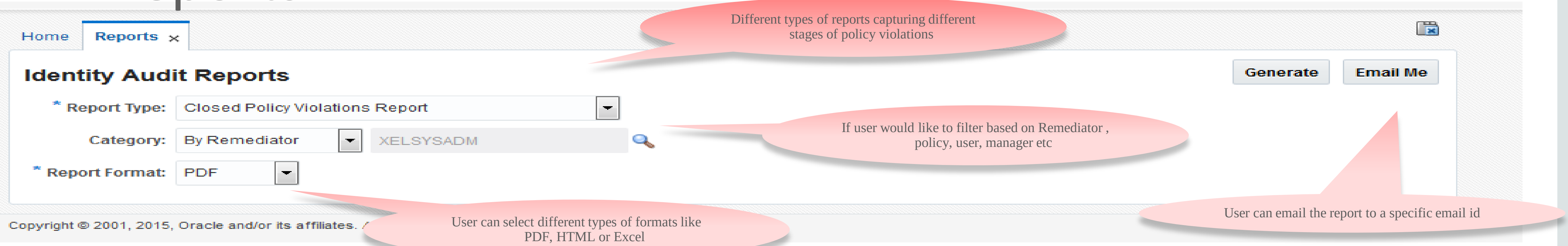
Display Name	Description	Action	Risk Summary	Comments
OUD on localhost(KVESTERDAL)				
Accounts Payable User				
Accounts Payable Administrator				

Rows Selected 1 | Columns Hidden 13

Detailed Information

Policy Name	Status	Remediator	Severity
Accounts Payable SoD Policy	Assigned	Xavier Hanel	🟩

IDA Reports



Identity Audit Reports

* Report Type: Closed Policy Violations Report

Category: By Remediator XELSYSADM

* Report Format: PDF

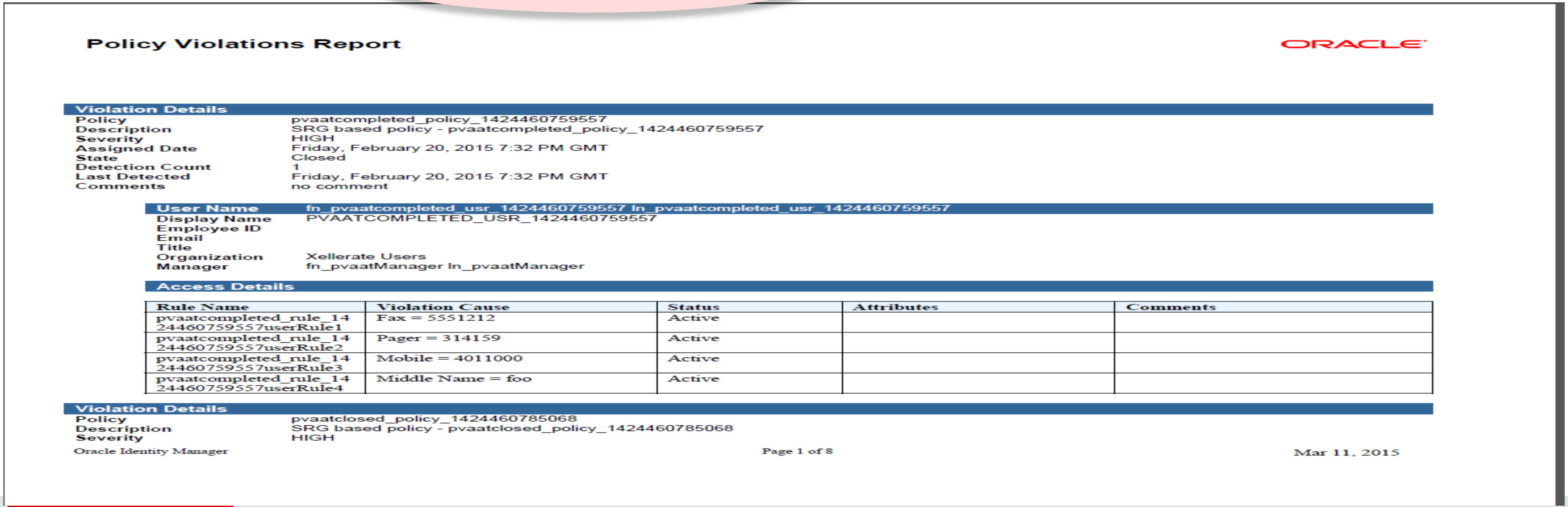
Copyright © 2001, 2015, Oracle and/or its affiliates.

Different types of reports capturing different stages of policy violations

If user would like to filter based on Remediator , policy, user, manager etc

User can select different types of formats like PDF, HTML or Excel

User can email the report to a specific email id



Policy Violations Report

Violation Details

Policy	pvaatcompleted_policy_1424460759557
Description	SRG based policy - pvaatcompleted_policy_1424460759557
Severity	HIGH
Assigned Date	Friday, February 20, 2015 7:32 PM GMT
State	Closed
Detection Count	1
Last Detected	Friday, February 20, 2015 7:32 PM GMT
Comments	no comment

User Name	fn_pvaatcompleted_usr_1424460759557 ln_pvaatcompleted_usr_1424460759557
Display Name	PVAATCOMPLETED_USR_1424460759557
Employee ID	
Email	
Title	
Organization	Xellerate Users
Manager	fn_pvaatManager ln_pvaatManager

Access Details

Rule Name	Violation Cause	Status	Attributes	Comments
pvaatcompleted_rule_1424460759557userRule1	Fax = 5551212	Active		
pvaatcompleted_rule_1424460759557userRule2	Pager = 314159	Active		
pvaatcompleted_rule_1424460759557userRule3	Mobile = 4011000	Active		
pvaatcompleted_rule_1424460759557userRule4	Middle Name = foo	Active		

Violation Details

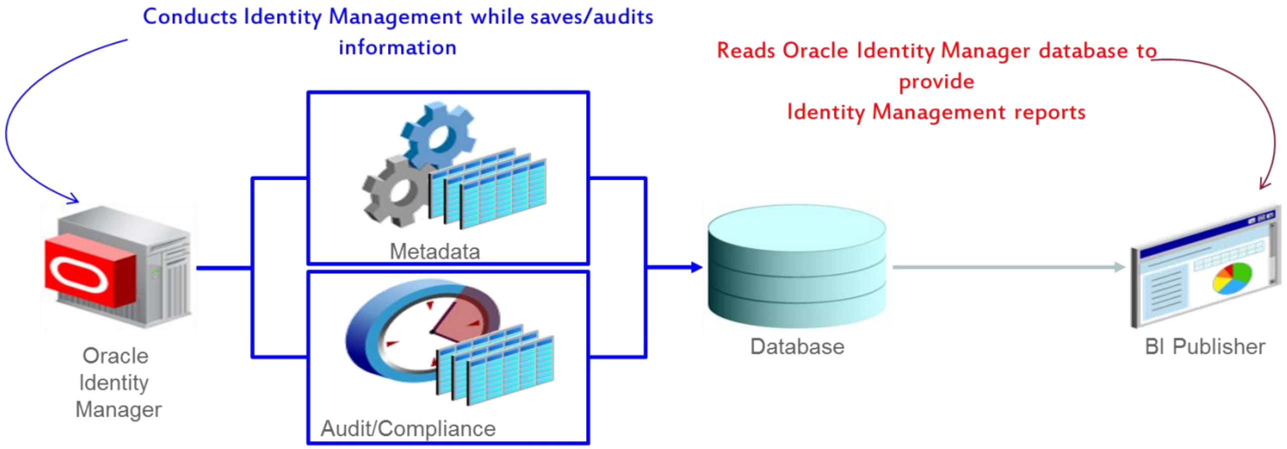
Policy	pvaatclosed_policy_1424460785068
Description	SRG based policy - pvaatclosed_policy_1424460785068
Severity	HIGH

Oracle Identity Manager Page 1 of 8 Mar 11, 2015

Audit and Reporting

Audit and Reporting

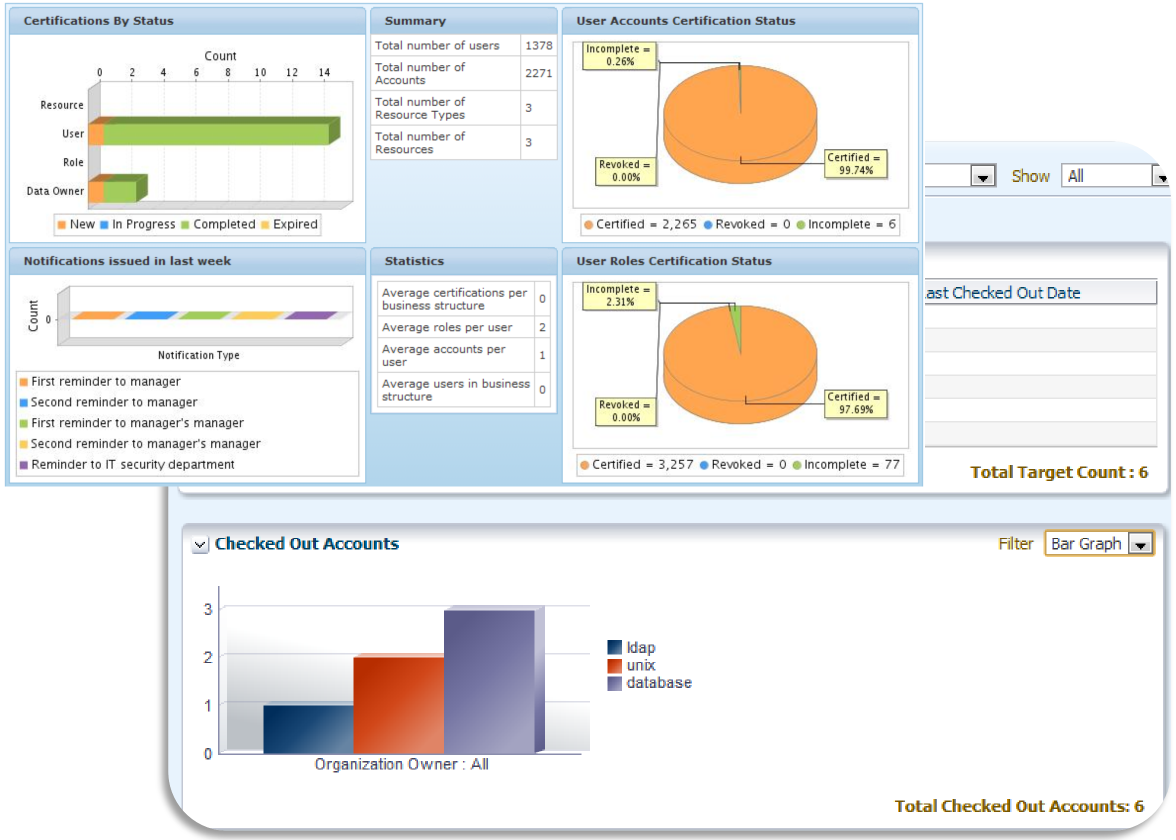
The audit and reporting life cycle steps


Conducts Identity Management while saves/audits information
Reads Oracle Identity Manager database to provide Identity Management reports
Metadata
Oracle Identity Manager
Audit/Compliance
Database
BI Publisher

- Oracle Identity Manager generates data
- The Oracle Identity Manager data is stored in a database
- The Oracle BI Publisher queries Oracle Identity Manager data to create reports. (with Ps3)

Audit and Reporting

Reports and Dashboards


Certifications By Status
Count
0
2
4
6
8
10
12
14
Resource
User
Role
Data Owner
🟧 New 🟦 In Progress 🟩 Completed 🟨 Expired
Notifications issued in last week
Count
0
Notification Type
🟧 First reminder to manager
🟦 Second reminder to manager
🟩 First reminder to manager's manager
🟨 Second reminder to manager's manager
🟪 Reminder to IT security department
User Accounts Certification Status
Incomplete = 0.26%
Revoked = 0.00%
Certified = 99.74%
● Certified = 2,265 ● Revoked = 0 ● Incomplete = 6
User Roles Certification Status
Incomplete = 2.31%
Revoked = 0.00%
Certified = 97.69%
● Certified = 3,257 ● Revoked = 0 ● Incomplete = 77
ast Checked Out Date
3
2
1
0
Organization Owner : All
ldap
unix
database

Summary

Total number of users	1378
Total number of Accounts	2271
Total number of Resource Types	3
Total number of Resources	3

Statistics

Average certifications per business structure	0
Average roles per user	2
Average accounts per user	1
Average users in business structure	0

Show All

Total Target Count : 6

Checked Out Accounts

Filter Bar Graph

Total Checked Out Accounts: 6

- Actionable dashboards for risk analysis and compliance
- 80+ OOTB reports providing a 360 deg.
  view of users' access
- Flexible deployment options, including
  ability to schedule report runs
- Publicly available schema

Audit and Reporting

OOB Reports – High Level Category

Access Policy Reports

- Access Policy Details
- Access Policy List by Role

Attestation, Request, and Approval Reports

- Approval Activity
- Attestation Process List
- Attestation Request Details
- Attestation Requests by Process
- Attestation Requests by Reviewer
- Request Details
- Request Summary
- Task Assignment History

User Reports

- User Profile History
- User Summary
- Users Deleted
- Users Disabled
- Users Unlocked

Role and Organization Reports

- Role Membership History
- Role Membership Profile
- Role Membership
- Organization Details
- User Membership History
- Account Activity In Resource
- Delegated Admins and Permissions by Resource
- Delegated Admins by Resource
- Entitlement Access List

Password Reports

- Password Expiration Summary
- Password Reset Summary
- Resource Password Expiration

Certification Reports

Exception Reports

- Fine Grained Entitlement Exceptions By Resource
- Orphaned Account Summary
- Rogue Accounts By Resource

Resource and Entitlement Reports

- Entitlement Access List History
- Financially Significant Resource Details
- Resource Access List History
- Resource Access List
- Resource Account Summary
- Resource Activity Summary
- User Resource Access History
- User Resource Access
- User Resource Entitlement
- User Resource Entitlement History

Hardware and Software

Engineered to Work Together